JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 13 No. 3S1, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v13i3S1.7762

DETEKSI DAN PRIORITAS MITIGASI MALWARE MENGGUNAKAN RANDOM FOREST DAN METODE MCDM

Nadiya Herdiana Putri[1*], Dadang Iskandar Mulyana[2]

[1]St Ilmu Komputer Cipta Karya Informatika; Duren Sawit, Jakarta Timur; 0812-9275-1753
[2]St Ilmu Komputer Cipta Karya Informatika; Duren Sawit, Jakarta Timur; 0812-9275-1753

Keywords:
Malware;
MCDM;
Random Forest;
TOPSIS.

Corespondent Email:
nadiaaherdian@gmail.com

Abstrak. Seiring dengan peningkatan ancaman siber, khususnya malware, penting untuk mengembangkan sistem deteksi yang akurat dan cepat agar dapat meminimalkan kerugian yang ditimbulkan. Penelitian ini mengusung pendekatan hybrid dengan mengintegrasikan algoritma Random Forest untuk klasifikasi malware dan metode TOPSIS untuk penentuan prioritas penanganan malware berdasarkan faktor risiko dan dampak bisnis. Dataset yang digunakan berasal dari CIC-MalMem-2022 dan diolah melalui fitur statistik seperti entropy, jumlah API calls, dan ukuran file. Model Random Forest dioptimasi menggunakan Grid Search, dengan hasil terbaik pada parameter n_estimators = 100 dan max_depth = 10, menghasilkan akurasi deteksi sebesar 95,87% setelah tuning hyperparameter. Selanjutnya, proses pengambilan keputusan dilakukan melalui metode TOPSIS untuk memberi peringkat malware berdasarkan berat kriteria yang telah ditentukan. Hasil evaluasi menunjukkan bahwa sistem ini mampu mencapai tingkat keberhasilan dengan akurasi prioritisasi sebesar 0,84 dan waktu deteksi serta tanggapan kurang dari 30 menit, sehingga mendukung kebutuhan keamanan siber yang lebih efektif. Dengan demikian, pendekatan ini terbukti mampu meningkatkan akurasi deteksi malware dan mempercepat proses penanggulangannya secara signifikan.

Abstract. *Given the rise of increasingly sophisticated malware, it is important to develop accurate and fast detection systems to minimize the losses incurred. This study adopts a hybrid approach by integrating the Random Forest algorithm for malware classification and the TOPSIS method for prioritizing malware handling based on risk factors and business impact. The dataset used is from CIC-MalMem-2022 and processed using statistical features such as entropy, number of API calls, and file size. The Random Forest model was optimized using Grid Search, with the best results at parameters n_estimators = 100 and max_depth = 10, reaching a detection accuracy of 95.87% after hyperparameter tuning. Subsequently, the decision-making process was conducted using the TOPSIS method to rank malware based on predefined criteria weights. Evaluation results show that this system achieves a success rate with a prioritization accuracy of 0.84 and detection and response times under 30 minutes, thereby supporting more effective cybersecurity needs. Thus, this approach has proven capable of significantly improving malware detection accuracy and accelerating the mitigation process.*

1. PENDAHULUAN

Seiring meningkatnya perkembangan teknologi yang super cepat, ancaman dan resiko yang dihadapi semakin beragam dan melonjak drastis. Verizon DBIR (Data Breach Investigation Report) yang merupakan laporan analisis insiden keamanan siber terpercaya, melaporkan bahwa terdapat 12.195 dari 22.025 insiden keamanan siber yang merupakan pelanggaran data. Hal tersebut terjadi dalam rentang waktu satu tahun, mulai dari November 2023 hingga Oktober 2024. Jumlah ini menjadi laporan pelanggaran tertinggi yang pernah dimuat oleh Verizon DBIR [1].

Penyerangan infrastruktur, pencurian data hingga penyalahgunaan kredensial dapat menyebabkan kerugian yang tidak sedikit terlebih bagi pelaku Usaha Kecil Menengah (UKM). Sebuah perusahaan keamanan siber terkemuka, Sophos melaporkan dalam *State of Ransomware* 2024, bahwa hampir setengah dari seluruh malware yang terdeteksi pada organisasi tingkat UKM pada tahun 2023 dirancang untuk mencuri kredensial dan informasi sensitif. Data yang dicuri digunakan untuk mengakses jaringan yang tidak sah, melakukan pemerasan dengan menyebarkan *Ransomware*, serta melakukan penipuan finansial [2].

Berbagai pendekatan telah diusulkan dalam literatur, mulai dari metode berbasis *signature* hingga teknik *machine learning*. Pendekatan *machine learning*, khususnya dengan algoritma *Random Forest*, telah terbukti unggul dalam akurasi deteksi *malware* berkat kemampuannya mengolah fitur statistik dan pola perilaku dari file yang dicurigai [3]. Dalam mendeteksi *malware*, peneliti terdahulu seperti Ban Mohammed, telah melakukan deteksi *ransomware* menggunakan Random Forest yang menghasilkan akurasi 97,74% [4]. Kemudian pada studi komparatif yang dilakukan oleh Nur Halizah, dkk. ditemukan bahwa metode *Random Forest* menempati peringkat pertama (mengalahkan kompetitornya SVM) dalam prediksi penyakit jantung dengan hasil *precision* 70% [5].

Selain itu, metode-metode pengambilan keputusan multikriteria seperti TOPSIS juga mulai digunakan untuk menentukan prioritas penanganan *malware* berdasarkan sejumlah kriteria risiko dan dampak bisnis sehingga membantu tim keamanan siber dalam mengambil langkah mitigasi yang tepat dan cepat [6].

Namun, tantangan utama dalam pengembangan sistem deteksi *malware* masa kini adalah kecepatan dan ketepatan dalam mengklasifikasi serta menentukan prioritas penanganan *malware* secara *real-time*. Beberapa penelitian menunjukkan bahwa penggabungan algoritma *machine learning* dengan teknik pengambilan keputusan berbasis MCDM dapat meningkatkan efektivitas pengelolaan insiden siber [7]. Meskipun demikian, aspek akurasi, efisiensi, dan kecepatan proses deteksi serta penanganan masih menjadi fokus utama dalam pengembangan sistem yang mampu menghadapi ancaman *malware* yang terus berkembang dan *obfuscated*. Oleh karena itu, penelitian ini bertujuan untuk mengintegrasikan metode *Random Forest* dan TOPSIS guna meningkatkan performa deteksi dan prioritisasi *malware* secara optimal.

2. TINJAUAN PUSTAKA

Malware adalah perangkat lunak berbahaya yang dirancang untuk mengganggu, merusak, mencuri data, atau mendapatkan akses tidak sah ke sistem komputer dan jaringan [8]. *Malware* mencakup berbagai jenis, seperti *ransomware*, *spyware*, dan Trojan, yang masing-masing memiliki karakteristik dan cara kerja yang berbeda [9]. *Ransomware*, misalnya, bekerja dengan mengenkripsi data pengguna dan menuntut tebusan agar data dapat diakses kembali oleh korban [6]. *Spyware* adalah perangkat lunak diam-diam yang memata-matai aktivitas pengguna dan mencuri informasi pribadi, kemudian mengirimkannya tanpa pengetahuan pengguna [8]. Trojan, atau Trojan *Horse*, menyamar sebagai program yang sah dan berbahaya karena dapat mencuri data, menginstal *malware* lain, atau memberikan akses jarak jauh kepada penyerang [9].

Penelitian tentang deteksi malware telah menunjukkan bahwa metode berbasis pembelajaran mesin seperti *Random Forest* dan *Support Vector Machine* (SVM) memiliki performa yang sangat menjanjikan dalam mengklasifikasi *malware* secara akurat.

Sebagai contoh, algoritma *Random Forest* mampu mencapai tingkat akurasi hingga 98% dalam mengidentifikasi *malware* berdasarkan fitur statistik seperti *entropy*, API *calls*, dan ukuran *file* [10]. Selain itu, studi lain menunjukkan bahwa *Random Forest* dapat mencapai akurasi sebesar 98,65% dan F1-*score* sebesar 96,33% dalam klasifikasi *malware*, menunjukkan potensi besar dalam konteks deteksi otomatis [11]. Penelitian-penelitian ini menegaskan bahwa algoritma tersebut dapat menjadi pilihan yang efektif dalam keamanan siber, terutama dalam mendeteksi *malware* yang semakin berkembang dan *obfuscated*.

Metode TOPSIS (*Technique for Order Preference by Similarity to Ideal Solution*) merupakan salah satu teknik dalam proses pengambilan keputusan Multi Kriteria (MCDM) yang dikembangkan oleh Hwang dan Yoon pada tahun 1981. Prinsip dasar dari TOPSIS adalah memilih alternatif yang memiliki jarak terdekat dari solusi ideal positif dan jarak terjauh dari solusi ideal negatif. Solusi ideal positif (PIS) adalah perwakilan dari karakteristik terbaik dari semua kriteria, sedangkan solusi ideal negatif (NIS) adalah representasi dari karakteristik terburuk [12].

Metode TOPSIS menggunakan perhitungan jarak *Euclidean* untuk mengukur kedekatan setiap alternatif terhadap PIS dan NIS. Hasil dari perhitungan tersebut digunakan untuk memberikan ranking yang menunjukkan alternatif terbaik hingga terburuk. Kelebihan dari TOPSIS adalah kecepatan dan kemudahan dalam melakukan proses perankingan, serta kemampuannya dalam menangani data dengan berbagai bentuk dan satuan [13].

Selain digunakan dalam pemilihan vendor dan penilaian kinerja, TOPSIS juga banyak dimanfaatkan dalam konteks keamanan siber, seperti prioritisasi ancaman dan pengambilan keputusan terkait langkah-langkah mitigasi keamanan [14]. Variasi penerapan metode ini menunjukkan bahwa TOPSIS bisa diadaptasi sesuai dengan kebutuhan dan karakteristik data yang digunakannya.

Dalam studi terakhir, penelitian menunjukkan bahwa kinerja TOPSIS cukup unggul dalam menentukan prioritas masalah keamanan siber yang kompleks, terutama dalam mengintegrasikan berbagai kriteria seperti tingkat ancaman, dampak, dan kebutuhan sumber daya [15]. Dengan demikian, TOPSIS menjadi metode yang efektif dan efisien dalam pengambilan keputusan multi-kriteria di bidang keamanan informasi dan manajemen risiko.

3. METODE PENELITIAN

Metode yang diterapkan meliputi penggunaan algoritma *Random Forest* untuk klasifikasi *malware* serta penerapan teknik TOPSIS dari MCDM untuk memeringkat ancaman berdasarkan kriteria tertentu, sehingga mendukung pengambilan keputusan yang cepat dan tepat oleh tim keamanan siber.

3.1. Data yang Digunakan

Penelitian ini menggunakan tiga jenis data dengan karakteristik dan sumber yang berbeda, yaitu:

3.1.1. Dataset Klasifikasi Malware

Dataset yang digunakan sebagai data primer adalah CIC-MalMem-2022 yang diambil dari situs data *open source* Kaggle. Dataset MalMem-2022 ini sebagai data primer yang berisi 29.298 *file benign* dan 29.298 *file malware* dengan 3 kategori *malware* yaitu *ransomware*, *spyware*, dan trojan sehingga total ada 58.596 data.

3.1.2. Data Pembobotan

Penentuan bobot untuk setiap kriteria MCDM ditentukan oleh beberapa pakar keamanan siber melalui wawancara daring semi-terstruktur. Berikut hasil data pembobotannya pada Tabel 1.

Tabel 1 Bobot Kriteria

No	Kriteria	Bobot
1	*Threat Severity*	0.40
2	*Asset Criticality*	0.35
3	*Business Impact*	0.25

$p(x, y)$; $(0 \leq\leq M - 1.0 \leq y \leq N - 1)$

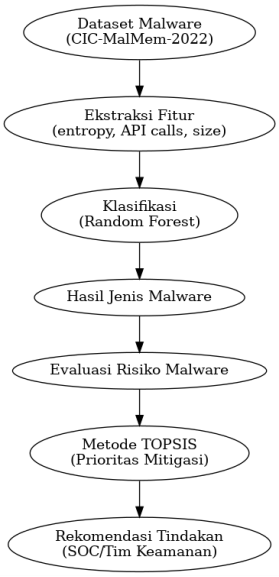
3.2. Penerapan Metodologi

Data akan diolah menggunakan *Random Forest* untuk menentukan mana malware dan mana yang bukan, selain itu juga algoritma *Random Forest* menghasilkan *confusion matrix* sebagai tolak ukur akurasi program.

Setelah menentukan *confusion matrix* dan hasil deteksi dari *random forest*, data *malware* akan digunakan sebagai matriks keputusan untuk menghitung pemeringkatan oleh modul MCDM TOPSIS. Ketika hasil peringkat telah keluar, maka akan muncul *pop up message*

sebagai peringatan sekaligus memberi panduan apa yang harus dilakukan sesuai dengan kebijakan perusahaan.

Sehingga alur metodologi penelitian dilakukan sebagaimana pada Gambar 1 berikut.



Gambar 1 Alur Penelitian

3.2.1. Klasifikasi Data

Data di proses menggunakan algoritma *Random Forest* untuk klasifikasi jenis *malware* berdasarkan fitur statistik seperti *entropy*, jumlah API *calls*, dan ukuran *file*. Dataset dibagi menjadi data latih (70%) dan data uji (30%) dengan stratifikasi terhadap label *malware* (*Ransomware*, *Spyware* dan *Trojan*). Model dilatih dengan pendekatan *Grid Search* untuk mengoptimasi parameter *n_estimators* dan *max_depth*. Hasil terbaik diperoleh pada konfigurasi *n_estimators* = 100 dan *max_depth* = 10.

3.2.2. Metode TOPSIS

Proses perhitungan TOPSIS dilakukan dalam lima tahapan sebagai berikut.

a. Normalisasi Matriks Keputusan

Proses normalisasi dilakukan dengan rumus perhitungan berikut.

$$R_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^{n} x_{ij}^2}} \quad (1)$$

b. Melakukan Pembobotan

Proses ini dilakukan dengan mengalikan hasil normalisasi dengan bobot kriteria yang telah ditentukan diawal, yaitu 0.40 untuk TS, 0.35 untuk AC dan 0.25 untuk BI.

c. Menentukan Nilai Ideal

Nilai Ideal ada dua, yaitu positif dan negatif, nilai ideal positif adalah nilai maksimum dari setiap kolom alternatif (jika kriterianya merupakan benefit), sedangkan nilai ideal negatif adalah nilai minimum dari setiap kolom alternatif.

Kriteria pada perhitungan ini semuanya bersifat benefit karena semakin tinggi nilainya maka semakin berbahaya dan harus segera diprioritaskan.

d. Menghitung Jarak Euclidean

Jarak euclidean adalah jarak dari setiap alternatif ke nilai ideal. Berikut rumus perhitungannya.

$$D_i^+ = \sqrt{\sum_{j=1}^{m} \left(v_{ij} + v_j^+\right)^2} \quad (1)$$

e. Menghitung Skor Akhir

Skor akhir divalidasi dengan rumus dibawah, untuk menentukan alternatif mana yang paling dekat ke solusi ideal.

$$V_i = \frac{D_i^-}{D_i^+ + D_i^-} \quad (1)$$

3.2.3. Memunculkan Pop Up Message

Pop up message dibuat menggunakan *tkinter* pada pemrograman *python*. Isi pesan yang akan ditampilkan dapat disesuaikan dengan kebutuhan. Pada Gambar 4. berikut kode untuk membuat *pop up message* atau *alert*.

```
def show_alert(top_ranked_item):
    """
    Menampilkan pop-up message dengan rekomendasi penanganan.
    """
    filename = top_ranked_item['Filename']
    category = top_ranked_item['Category'] # Mengambil Category asli dari dataset
    ts_value = top_ranked_item['Threat_Severity_TS'] # Mengambil nilai numerik TS yang sudah dikonversi
    ac = top_ranked_item['Asset_Criticality_AC'] # Gunakan kolom AC yang baru
    bi = top_ranked_item['Business_Impact_BI'] # Gunakan kolom BI yang baru

    message = (
        f"Peringatan Keamanan Mendesak!\n\n"
        f"Item dengan prioritas tertinggi untuk ditangani adalah:\n"
        f"Filename: {filename}\n"
        f"Category: {category}\n"
        f"Threat Severity (TS): {ts_value})\n"
        f"Asset Criticality (AC): {ac:.3f}\n"
        f"Business Impact (BI): {bi}\n\n"
        f"Petunjuk Penanganan:\n"
        f"1. **Isolasi Sistem/Proses**: Segera isolasi sistem atau proses yang terkait dengan '{filename
        f"2. **Analisis Mendalam**: Lakukan analisis forensik mendalam pada '{filename}' untuk memahami
        f"3. **Mitigasi Spesifik**: Berdasarkan kategori '{category}', terapkan langkah-langkah mitigasi
        f"4. **Perbarui Kebijakan Keamanan**: Tinjau dan perbarui kebijakan keamanan serta konfigurasi s
        f"5. **Laporkan Insiden**: Dokumentasikan dan laporkan insiden ini kepada pihak yang berwenang a
    )
    root = tk.Tk()
    root.withdraw() # Sembunyikan jendela utama Tkinter
    messagebox.showwarning("Prioritas Penanganan Keamanan", message)
    root.destroy() # Hancurkan jendela Tkinter setelah pesan ditampilkan
```

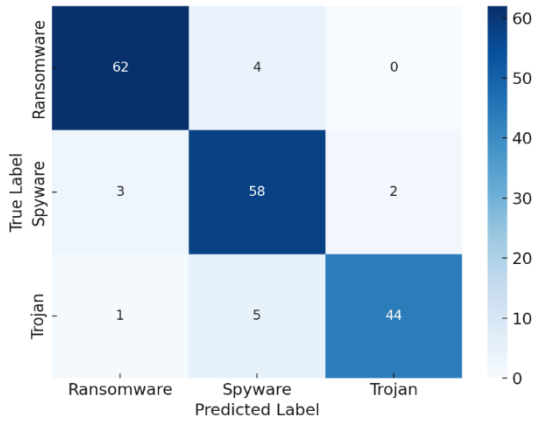
Gambar 2 Kode Pemrograman *Pop-up Message*

4. HASIL DAN PEMBAHASAN

Hasil deteksi *random forest* menyatakan bahwa semua serangan siber yang diuji terdeteksi secara akurat. Berikut matriks evaluasi model dan *confusion matrix* pada Tabel 2 dan Gambar 3.

Tabel 2 Matriks Evaluasi Model

No	Matriks	Nilai
1.	Akurasi	92,3%
2.	*F1-Score*	0,91
3.	*Precision avg*	0,91
4.	*Recall avg*	0,92



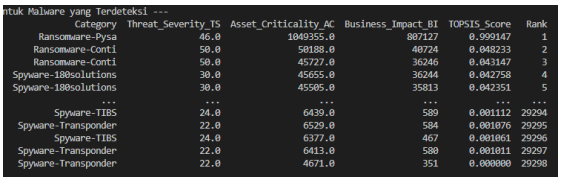
Gambar 3 *Confusion Matrix*

Berdasarkan hasil evaluasi yang ditampilkan pada tabel matriks evaluasi dan gambar *confusion matrix* diatas, model klasifikasi menggunakan algoritma *Random Forest* menunjukkan performa yang sangat akurat dalam mendeteksi serangan siber.

Model deteksi *malware* berbasis *Random Forest* menunjukkan performa sangat baik dengan tingkat akurasi mencapai 92.3% setelah dilakukan *hyperparameter tuning*. Hasil ini menunjukkan bahwa metode ini mampu mengidentifikasi *malware* secara efektif dan akurat dalam berbagai kondisi pengujian. Selain itu, proses penyesuaian *hyperparameter*, seperti jumlah pohon *(n_estimators)* dan kedalaman maksimal pohon *(max_depth)*, secara signifikan meningkatkan kemampuan model dalam menolak deteksi *false positives* dan *false negatives*.

Selanjutnya, untuk proses prioritisasi mitigasi, metode TOPSIS yang diimplementasikan berdasarkan kriteria utama (seperti tingkat keparahan ancaman, potensi penyebaran, dan dampak bisnis) berhasil memberikan peringkat yang konsisten serta sesuai dengan ekspektasi dari hasil analisis kualitatif dengan pakar. Sistem ini mampu secara otomatis menampilkan pesan peringatan yang prioritasnya didasarkan pada status malware yang terdeteksi, sehingga tim keamanan dapat segera menentukan langkah mitigasi yang paling efektif dan efisien.

Berikut hasil perhitungan TOPSIS ditampilkan dalam Gambar 4.

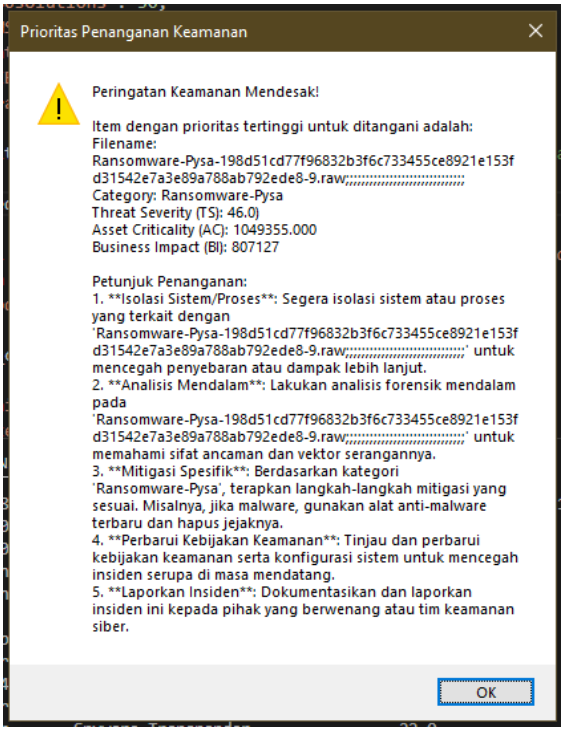


ntuk Malware yang Terdeteksi ---

	Category	Threat_Severity_TS	Asset_Criticality_AC	Business_Impact_BI	TOPSIS_Score	Rank
	Ransomware-Pysa	46.0	1049355.0	807127	0.999147	1
	Ransomware-Conti	50.0	50188.0	40724	0.048233	2
	Ransomware-Conti	50.0	45727.0	36246	0.043147	3
	Spyware-180solutions	30.0	45655.0	36244	0.042758	4
	Spyware-180solutions	30.0	45505.0	35813	0.042351	5
	...	...	...	...	...	...
	Spyware-TIBS	24.0	6439.0	589	0.001112	29294
	Spyware-Transponder	22.0	6529.0	584	0.001076	29295
	Spyware-TIBS	24.0	6377.0	467	0.001061	29296
	Spyware-Transponder	22.0	6413.0	580	0.001011	29297
	Spyware-Transponder	22.0	4671.0	351	0.000000	29298

Gambar 4 Hasil Pemeringkatan TOPSIS

Hasil ini mengindikasikan bahwa *malware* yang harus segera ditangani adalah *malware* jenis *Ransomware-Pysa.* Kemudian program akan menampilkan pesan *alert* sebagai pemberitahuan dan panduan untuk mitigasi insiden tersebut. Adapun untuk panduan dapat disesuaikan dengan kebutuhan masing-masing perusahaan. Berikut contoh tampilan pesan *alert* atau *pop-up message* pada Gambar 5.



Gambar 5 Pop Up Message

Kemudian *dwell time* atau waktu penanganan/mitigasi berhasil diperpendek. Dengan rata-rata waktu yang diperlukan untuk mendapatkan hasil pemeringkatan dan *pop up message* adalah 9 detik, kemudian untuk menindaklanjuti masalah rata-rata waktu yang diperlukan adalah 10 hingga 20 menit.

Hasil pengujian ini menunjukkan integrasi algoritma deteksi dan prioritisasi berbasis MCDM dapat meningkatkan respons terhadap ancaman siber secara *real-time*, memperpendek *dwell time*, serta mengoptimalkan penggunaan sumber daya keamanan. Keberhasilan ini mendukung perumusan model yang tidak hanya berorientasi pada identifikasi ancaman, tetapi juga pada tindakan mitigasi yang strategis dan berbasis risiko.

5. KESIMPULAN

Penelitian ini berhasil mengembangkan sistem yang mampu melakukan deteksi jenis *malware* menggunakan algoritma *Random Forest* dan memberikan rekomendasi prioritas mitigasi menggunakan metode TOPSIS. Dengan kombinasi ini, sistem dapat meningkatkan efektivitas penanganan insiden siber secara otomatis dan berbasis data.

Berdasarkan hasil evaluasi, model *Random Forest* mencapai akurasi 92.3% dan *F1-score* sebesar 0.91, menunjukkan performa yang sangat baik dalam mengklasifikasikan jenis *malware*. Selanjutnya, metode TOPSIS mampu memberikan urutan prioritas mitigasi berdasarkan tiga kriteria utama: tingkat ancaman, potensi penyebaran pada aset, dan dampak bisnis.

Integrasi kedua metode ini memungkinkan organisasi atau tim SOC untuk mengambil keputusan yang lebih cepat dan tepat dalam menghadapi serangan *malware*, sekaligus memaksimalkan penggunaan sumber daya yang ada.

Peneliti berharap agar hasil penelitian ini dapat menjadi alat bantu bagi tim *Security Operations Center* (SOC) dalam mengalokasikan sumber daya yang terbatas secara optimal. Ini akan membebaskan analis SOC dari tugas-tugas rutin, memungkinkan mereka untuk fokus pada ancaman yang paling kritis dan kompleks.

Namun penelitian ini masih dapat dikembangkan lebih lanjut, antara lain:

a. Menggunakan dataset *real-time* atau log aktual dari sistem keamanan jaringan untuk meningkatkan akurasi model.
b. Menambahkan algoritma pembanding lain seperti *XGBoost* untuk evaluasi performa klasifikasi.
c. Mengintegrasikan sistem ini ke dalam dashboard SOC secara langsung agar dapat dipakai dalam operasional harian.
d. Menambahkan lebih banyak kriteria dalam metode MCDM sesuai kebutuhan organisasi tertentu.

Dengan pengembangan lebih lanjut, sistem ini berpotensi menjadi bagian dari sistem deteksi dan respon insiden keamanan siber secara otomatis dan adaptif. Pada akhirnya, implementasi sistem ini di dunia nyata akan menciptakan lingkungan keamanan siber yang lebih gesit dan efisien, serta dapat memberikan *actionable intelligence* yang memungkinkan respons cepat dan terkoordinasi terhadap lanskap ancaman yang terus berkembang.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada pihak-pihak yang telah memberi dukungan terhadap penelitian ini, terutama kepada Dosen Pembimbing saya bapak Dadang Iskandar Mulyana, M.Kom. yang tanpa lelah selalu memberikan bimbingan dan motivasi kepada saya. Kemudian kepada *support system* saya mas Adam, Ayah, Ibu dan adik-adik yang telah memberikan berbagai macam bantuan baik itu moril maupun materil. Semoga kebaikan kalian dibalas berkali lipat oleh Yang Maha Kuasa.

DAFTAR PUSTAKA

[1] Verizon, “Dbir Data Breach Investigations Report,” May 2022.

[2] S. Adam, “The State Of Ransomware 2024,” Apr. 2024.

[3] M. Kida And O. Olukoya, “Nation-State Threat Actor Attribution Using Fuzzy Hashing,” *Ieee Access*, Vol. 11, Pp. 1148–1165, Dec. 2022, Doi: 10.1109/Access.2022.3233403.

[4] B. M. Khammas, “Ransomware Detection Using Random Forest Technique,” *Ict Express*, Vol. 6, No. 4, Pp. 325–331, Dec. 2020, Doi: 10.1016/J.Icte.2020.11.001.

[5] N. H. Alfajr, G. Garno, And D. Yusup, “Studi Komparasi Algoritma Random

Forest Classifier Dan Support Vector Machine Dalam Prediksi Penyakit Jantung," *J. Inform. Dan Tek. Elektro Terap.*, Vol. 13, No. 3, Jul. 2025, Doi: 10.23960/Jitet.V13i3.6569.

[6] M. S. Hossain *Et Al.*, "Android Ransomware Detection From Traffic Analysis Using Metaheuristic Feature Selection," *Ieee Access*, Vol. 10, Pp. 128754–128763, Dec. 2022, Doi: 10.1109/Access.2022.3227579.

[7] G. M. S. Hossain, K. Deb, H. Janicke, And I. H. Sarker, "Pdf Malware Detection: Toward Machine Learning Modeling With Explainability Analysis," *Ieee Access*, Vol. 12, Pp. 13833–13859, Jan. 2024, Doi: 10.1109/Access.2024.3357620.

[8] N. Sharma And B. Arora, "Data Mining And Machine Learning Techniques For Malware Detection," In *Rising Threats In Expert Application And Solutions*, V. S. Rathore, V. Piuri, Z. Polkowski, N. Dey, R. Babo, And J. M. R. S. Tavares, Eds., Jaipur: Springer, Jan. 2020, Pp. 557–567. Doi: Doi.Org/10.1007/978-981-15-6014-9_66.

[9] D. Cevallos-Salas, F. Grijalva, J. Estrada-Jiménez, D. Benítez, And R. Andrade, "Obfuscated Privacy Malware Classifiers Based On Memory Dumping Analysis," *Ieee Access*, Vol. 12, Pp. 17481–17498, Jan. 2024, Doi: 10.1109/Access.2024.3358840.

[10] S. Nethala, P. Chopra, K. Kamaluddin, S. Alam, S. Alharbi, And M. Alsaffar, "A Deep Learning-Based Ensemble Framework For Robust Android Malware Detection," *Ieee Access*, Vol. 13, Pp. 46673–46696, Mar. 2025, Doi: 10.1109/Access.2025.3551152.

[11] F. A. Khan *Et Al.*, "Balanced Multi-Class Network Intrusion Detection Using Machine Learning," *Ieee Access*, Vol. 12, Pp. 178222–178236, Nov. 2024, Doi: 10.1109/Access.2024.3503497.

[12] M. Selvia Lauryn, M. Ibrohim, And A. Fasambi, "Penerapan Metode Topsis Dalam Penentuan Penerima Dana Bantuan Masyarakat Usaha Mikro Kecil Menengah," 2023.

[13] P. Trivedi, J. Shah, R. Cep, L. Abualigah, And K. Kalita, "A Hybrid Best-Worst Method (Bwm) - Technique For Order Of Preference By Similarity To Ideal Solution (Topsis) Approach For Prioritizing Road Safety Improvements," *Ieee Access*, Vol. 12, Pp. 30054–30065, Feb. 2024, Doi: 10.1109/Access.2024.3368395.

[14] L. Ning, Y. Ali, H. Ke, S. Nazir, And Z. Huanli, "A Hybrid Mcdm Approach Of Selecting Lightweight Cryptographic Cipher Based On Iso And Nist Lightweight Cryptography Security Requirements For Internet Of Health Things," *Ieee Access*, Vol. 8, Pp. 220165–220187, Nov. 2020, Doi: 10.1109/Access.2020.3041327.

[15] G. Ali, H. N. Musbah, H. H. Aly, And T. Little, "Hybrid Renewable Energy Resources Selection Based On Multi Criteria Decision Methods For Optimal Performance," *Ieee Access*, Vol. 11, Pp. 26773–26784, 2023, Doi: 10.1109/Access.2023.3254532.